Privacy Protection of Base Station in WSN's

Gaddam Uday[1], Raghupathi[2], K.Praveen Kumar [3]

[1,2,3]*Department of Computer Science and Engineering,*
Chaithanya Institute of Technology and Science, warangal, INDIA

Abstract: Location privacy in wireless sensor networks has gained a wide concern. Particularly, the location privacy of base station requires ultimate protection due to its crucial position in wireless sensor networks. In this paper, we propose an efficient scheme, consisting of anonymous topology discovery and intelligent fake packet injection (IFPI), to protect the location privacy of base station. Anonymous topology discovery eliminates the potential threats against base station within topology discovery period. On the other hand, IFPI enhances privacy protection strength during data transmission period. Under given conditions, comprehensive simulations demonstrate that our scheme significantly improves privacy strength compared with existing strategies.

Index Terms: Location Privacy; Base Station.

I. INTRODUCTION

Privacy is one of the most important problems in wireless sensor networks due to the open nature of wireless communication, which makes it very easy for adversaries to eavesdrop. Privacy in sensor networks is divided into two categories: content privacy, which concerns with the content of data packets, and transactional privacy, which focuses on information about the traffic features (such as carrier frequency, message rate and routing) [2]. Although content privacy can be protected by strong encryption and authentication mechanisms, sensor networks suffer from malicious traffic analysis. In this paper, we study the problem of location privacy.

A wireless sensor network typically consists of a large number of resource-constrained sensors, e.g. MICA2 motes, and a single base station (BS), e.g. PC-caliber gateway [3]. BS is used to manage and monitor the behavior of sensor nodes. The failure of BS will lead to collapse of the entire sensor network. An adversary would be eager to locate BS and perform further physical attack. Imagine a sensor network used for military purpose, BS collects information of the battlefield from sensors. If the location of BS is exposed to the enemy, this information channel will probably be destroyed. Thus, BS demands ultimate protection on its location privacy.

There are generally two ways for an adversary to locate BS: traffic-analysis and packet-tracing. The idea of trafficanalysis is that sensors near BS forward a greater volume of packets than sensors further away from BS [3]. An adversary is able to deduce the location of BS based on the traffic densities of various locations. By packet-tracing, an adversary infers a transmission link when he overhearstwo consecutive packets transmitted by adjacent nodes. Then he performs hop-by-hop tracing towards BS. Packet-tracing attack is more efficient than traffic-analysis attack for the adversary [4]. Therefore, we focus on the countermeasures against the packet-tracing attack.

The entire lifetime of a wireless sensor network can be divided into two kinds of operational phases: topology discovery and data transmission [5]. Most previous work deal with the location privacy in the data transmission period. However, they ignore the potential threats involved in the topology discovery period. Here we propose an anonymous topology discovery mechanism to eliminate the potential threats in the first period. Besides, we apply fake packet injection to protect the location privacy of BS in the data transmission period. Different from previous fake packet injection approaches, we consider the optimization issue and introduce an intelligent injection scheme to enhance the privacy strength. With the above two countermeasures, we present a complete solution for the location privacy of BS throughout the entire lifetime of wireless sensor networks.

The remainder of the paper is organized as follows. Section II Locationprivacy Routing Protocol (LPR). In Section III System Model. Section IV presents the results of experiments, and then we draw the conclusion in Section V.

II. LOCATIONPRIVACY ROUTING PROTOCOL (LPR)

Sensor network technologies promise drastic enhancement in automatic data collection capabilities through efficient deployment of small sensing devices. A sensor network typically consists of a large number of resource-constrained sensor nodes. Each node acts as an information source, collecting data samples from its environment and transporting data to a receiver via a multi-hop network, in which each node performs the routing function. With the availability of cheap wireless technologies and micro sensing devices, sensor networks are expected to be widely deployed in the near future. The open nature of wireless communication makes it easy for attackers to eavesdrop or inject data packets in a sensor network. Furthermore, unlike other wireless networks composed of mobile devices such as laptops and PDA's with human presence, sensor networks are usually deployed in open areas, where unattended sensor nodes lack physical protection. This means attackers will encounter much fewer obstacles when attacking a sensor network.

Privacy in sensor networks may be classified into two categories: content privacy and contextual privacy. Threats against content privacy arise due to the ability of adversaries to observe and manipulate the content of packets sent over a sensor network. This type of threats is countered by encryption and authentication. However, even after strong encryption and authentication mechanisms are applied, wireless communication media still exposes contextual information about the traffic carried in the network. For example, an adversary can deduce sensitive information from a sensor network by eavesdropping the network traffic and analyzing the traffic patterns. In particular, the location information about senders/receivers may be derived based on the directionof wireless communications. In this paper, we focus on the protection of location privacy for the receiver (or the base station) in sensor networks.

It is very important to protect the receiver's location privacy in a sensor network. First, in many sensor networks, the receiver is the most critical node of the whole network, as the responsibility of the receiver (i.e., the base station) is to collect data from all sensors. Since all sensors send data to a single node (the receiver), this creates a single point of failure in thenetwork. A sensor network can be rendered useless by taking down its receiver. Second, in some scenarios, the receiver itselfcan be highly sensitive. Imagine a sensor network deployed ina battlefield, where the receiver is carried by a soldier. If the location of the receiver is exposed to adversaries, the soldier will be in great danger.

There are several ways that an adversary can trace the location of a receiver. First, an adversary can deduce the location of the receiver by analyzing the traffic rate. This traffic-analysis attack is introduced and studied. The basic idea is that sensors near the receiver forward a greatervolume of packets than sensors further away from the receiver.By eavesdropping the packets transmitted at various locations in a sensor network, an adversary is able to compute the traffic densities at these locations, based on which it deduces the location of or the direction to the receiver. However, to perform the traffic-rate analysis, an adversary has to stay at each location long enough such that sufficient data can be gathered for computing the traffic rate. This process takes long time as the adversary moves from location to location. Second, an adversary can reach the receiver by following the movement of packets. This packet-tracing attack is first studied in, where the sender's location privacy, instead of the receiver's, is considered. In this attack, an equipped adversary can tell the location of the immediate transmitter of an overheard packet, and therefore he is able to perform hop-by-hop trace towards the original data source. We will show that the technique of packet tracing can be used to locate the receiver as well (Section III). Because the packet-tracing attack does not have to gather traffic-rate information, it allows an adversary to move quickly from location to location towards the receiver.

The packet-tracing attack may even be able to trace a mobile receiver due to its fast response, whereas the slow response of the traffic-analysis attack makes it unsuitable for such a task. In this paper, we focus on studying the defense measures against the packet-tracing attack.

When a traditional single-path routing protocol is used, a sensor network is extremely vulnerable to the packet-tracing attack, as the routing paths are fixed and point to the receiver. By eavesdropping the packet transmission, an adversary is able to move one hop along the shortest path towards the receiver for each packet overheard. In order to protect the receiver's location privacy, we propose a couple of countermeasures against the packettracing attack. First, we propose a new location-privacy routing protocol, called LPR, to provide path diversity. Second, we combine this routing protocol with fake packet injection to minimize the information that an adversary can deduce from the overheard packets about the direction towards the receiver.

Under such a protection scheme, an adversary can hardly distinguish between real packets and fake packets, or tell which direction is towards the receiver. Defending against the packet-tracing attack is a challenging problem. Cryptography does not help because the adversary deduces information simply by overhearing and following the radio transmissions. In order to remove the directional property in the movement of packets destined for a receiver, a considerable number of obfuscating transmissions have to be made. Path diversity provided by LPR inevitably leads to longer routing paths, and transmitting fake packets consumes extra energy. The stronger the protection for the receiver is required, the higher the overhead will be. To address the overhead problem, we design our system in such a way that one can easily tune the tradeoff between the protection strength and the overhead introduced in the network. It should also be noted that, if the security of the receiver is of great importance, overhead may be a price that one has to pay even in sensor networks, when better alternatives do not exist.

Many routing protocols establish a single path from each source node to the receiver. One of such protocols is described as follows. Each time the receiver moves to a new location, it broadcasts a beacon packet in the network. When a node receives a beacon for the first time, it forwards the beacon to its neighbors by a local broadcast. The beacon roughly follows a shortest-path tree to all sensors, which record their parents as the next hops to the receiver. Data packets will then follow the reverse direction of the broadcast tree towards the receiver. This procedure is similar to the interest propagation phase and the data propagation phase in the directed diffusion scheme, where ”gradients” from each node towards the receiver are first built before data packets can be routed. As explained in the introduction, single-path routing is vulnerable to thepacket-tracing attack.

For the location information of sensors, Random walk can efficiently preserve sensor's location privacy. A message is randomly forwarded from source, while it does not expose any information about the source. Actually, an adversary cannot know which random path is the accurate direction. So he cannot find the location of source and possibly reach an unknown sensor. But a pure random walk scheme is not secure for preserving private information of the location. In addition, it can be shown that a pure random walk tends to stay around the real source. Phantom Routing is proposed in, which is one of random walk approaches. The phantom routing is used to transmit information from the location of the panda to the sink for preserving its location privacy. Firstly, a message is randomly forwarded a few steps from data source. And then, the messageis being delivered through flooding or single path routing to base station. Fig.1 shows the phantom flooding scenario.

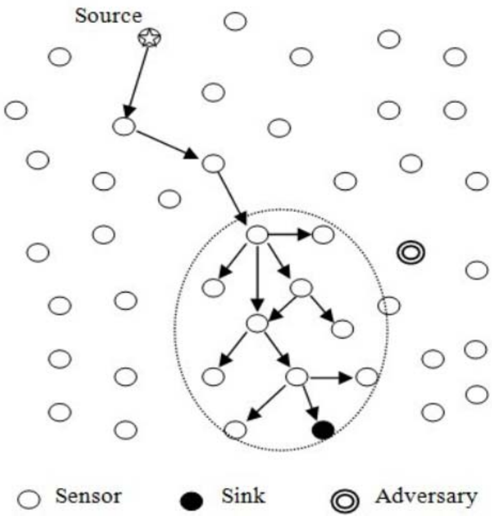


Fig.1. Phantom Flooding Protocol

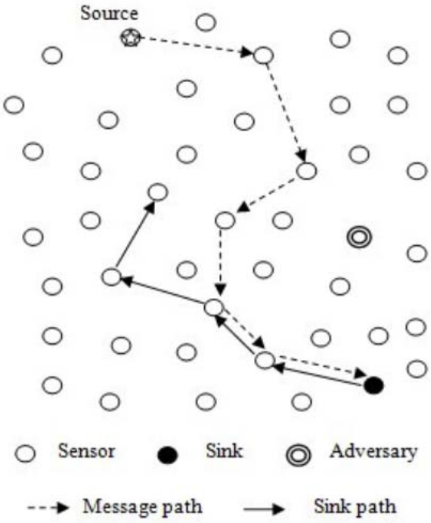


Fig.2. Message Randomly Walk and Follow Receptor Path

In order to prevent eavesdropper from gaining the location of a source, Greedy Random Walk scenario is proposed. And it is vividly shown in Fig.2. Firstly, it is initiated a random path with a given number of hops from the sink. Then each sensor on the path receives message as a receptor. Each message is randomly forwarded from a source until it reaches a receptor. And then themessage is forwarded to the sink through the pre-established path. However, an adversary still possibly backtrace to a sensor. And if an eavesdropper has the ability to monitor the whole sensor network, he may observe and analyze all traffic transmitted in the wireless sensor network. And then he will find that the traffic is higher than other sensors in this path. As a result, the eavesdropper may find the pre-established path and forward to base station through the pre-established path in that point. So it may threaten the safety of the base station. In our scheme, it can efficiently prevent an eavesdropper from finding the location information of source or base station and threatening the safety of sensors.

In order to facilitate the discussion and analysis of source location privacy in wireless sensor networks, we select the Random Walk and the Greedy Random Walk. But they do not efficiently prevent the adversary from finding the location information of source or base station. So we proposed a Local Protected Net scheme to preserve private location information.

III. SYSTEM MODEL

3.1 Network Model

Sensor networks consist of a number of different types of sensor nodes that have been deployed to monitor environment or collect data and send information to the sink in an area. In sensor networks, every sensor sends data to its neighboring nodes within its radio range. In this paper, we assume that all of sensors have roughly the same capabilities, power sources and expected lifetimes. And sensor nodes are evenly deployed in the sensor network and do not move after being deployed. When a sensor node monitors an object, the node will send a message to a base station. And a message is forwarded through certain routing strategies adopted the sensor networks. Moreover, we assume that a base station is deployed in the network and collects event data with greater computational capabilities.

3.2 Adversary Model

We assume that an adversary is a motivated and funded attacker whose objective is to learn sensitive location-based information in various kinds of wireless sensor networks. The adversary has unbounded energy resource, adequate computation capability and sufficient memory for data storage. And the adversary can observe and eavesdrop on the information in a limited range. Although the adversary can eavesdrop on the message between nearby sensor nodes to backtrace to a parent node, the adversary cannot determine the content of the message that is encrypted by secret keys. We assume that the adversary stay nearby the base station or the sink, where it is guaranteed that a large number of packets will arrive eventually. The adversary is constantly monitoring and eavesdropping. But the adversary doesn't know the exact location information of base station. When the eavesdropper monitors a message, he knows which node among the neighborhood sent that message and will move to the transmitting node. If the eavesdropper does not monitor any message for a certain time, he will stay or go back one step and keep monitoring. The adversary repeats this process until he reaches the source. Then the adversary can know the location information of source node.

Besides, the adversary can monitor the different transmission rates between the nodes and select the correct backtracking routing. And the eavesdropper may observe the correlation in transmission times between a node and its neighbors, attempting to deduce a routing path.

3.3. Local Protected Net Scheme

In this section, we propose a scheme for preserving location privacy. We assume that the contents of all transmitted data packets are encrypted by secret keys so that the adversary cannot gain the content of transmitted packets and find the location of sensors. Many key pre-distribution protocols can be used for our purpose. So the adversary cannot use the content to trace the object. The scheme can successfully make adversaries stay away from the base station or the source node. Besides, the method can effectively make trade-offs between privacy, communication cost and latency.

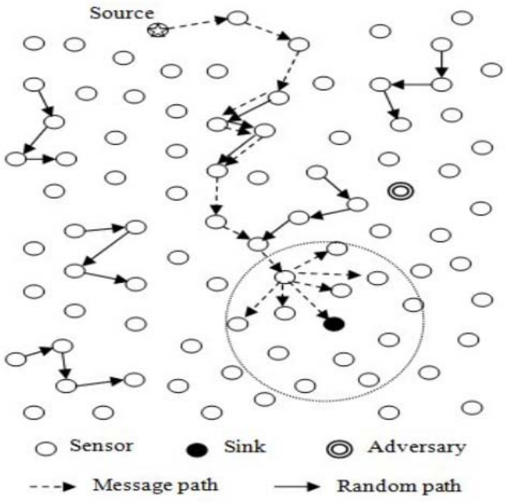
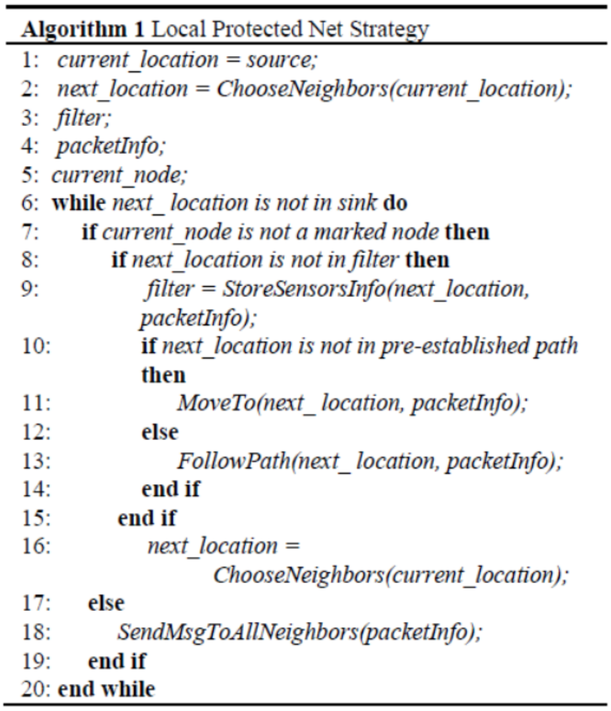


Fig.3. Local Protected Net Protocol



```
Algorithm 1 Local Protected Net Strategy
current_location = source;
next_location = ChooseNeighbors(current_location);
filter;
packetInfo;
current_node;
while next_ location is not in sink do
    if current_node is not a marked node then
        if next_location is not in filter then
            filter = StoreSensorsInfo(next_location,
            packetInfo);
            if next_location is not in pre-established path
            then
                MoveTo(next_ location, packetInfo);
            else
                FollowPath(next_ location, packetInfo);
            end if
        end if
            next_location =
                    ChooseNeighbors(current_location);
    else
        SendMsgToAllNeighbors(packetInfo);
    end if
end while
```

Fig.4. Local Protected Net Algorithm

In order to preserve information of location privacy, we propose a Local Protected Net scheme to address this problem. Firstly, the base station broadcasts special information to its neighbors which are marked by a special sign. So several marked nodes around the base station compose a special net, called Local Protected Net (LPN). And we initiate random paths which consist of a given number of hops in wireless sensor network. Sensors which are located on each random path will serve as the receptors. And sensors in the same path can transmit a data by a pre-established direction. Then a packet is randomly forwarded from a source until it reaches a receptor. At that point, the packet is forwarded through the pre-established path and reaches the end of this path. And then the packet is randomly forwarded again until it reaches the Local Protected Net. Meanwhile, when a node in LPN receives a packet, it will broadcast the packet and a special sign to its neighbors which include the base station. Fig.3 illustrates the basic idea of Local Protected Net.

However, it is possible that a packet may forward to one of its previous hop's neighbors or preestablished paths. So such that forwarding scheme is not good since the random walk does not make much progress. To solve this problem, we mark each pre-established path by a given number that each member knows in the path. Besides, the sensor nodes have its filter pool and store the forwarding packet information in the filter. When a sensor randomly chooses next hop from its neighbors, it should check whether the neighbor has been already in the filter. If the neighbor isn't in the filter, the sensor will broadcast the next node's ID to other sensor nodes. Then other nodes store the next sensor's ID in the filter.

In Fig.4 shows a packet will be forwarded to base station by Local Protected Net method. The packet is sent from the source that randomly chooses its neighbors as the next hop. Then the packet is sent to the next node. If the packet is not in the filter, the filter will store the information of the packet in this node. If the next node includes a pre-established path, the packet will follow this path and the filter will record the information about the packet in this path. Every node follows the rule to send the packet until it reaches the local protected net. And then, a node in LPN receives the packet and broadcast the packet to its neighbors with a special sign.

Note that it is efficient to preserve the sensor location privacy in our scheme. On the one hand, thepacket is randomly forwarded so that it is difficult to detect a packet by an eavesdropper. Even though an eavesdropper happens to detect a packet, the next packet is unlikely to follow the same path, thus rendering the previous observation useless. On the other hand, when a packet is transmitted in the protected net, an adversary cannot distinguish the correct direction or the incorrect one.

IV. CONCLUSION

In this paper, we proposed anonymous topology discovery and intelligent fake packet injection to protect the location privacy of BS. On one hand, we randomly choose a pseudo BS that initiates topology discovery to conceal the location of the real BS. On the other hand, we introduce an intelligent injection scheme to optimize existing fake packet injection method. Comprehensive experiments prove that our scheme provides stronger privacy protection than previous fake packet injection scheme by about two times.

For future work, we will consider a more powerful adversary model that has multiple and cooperative adversaries, and a more complex communication model, in which packetdelivery period is not constant.

REFERENCES

[1] Xinfeng Li, Xiaoyuan Wang, Nan Zheng, Zhiguo Wan, Ming Gu, "Enhanced Location Privacy Protection of Base Station in Wireless Sensor Networks", vol. 10, no. 4, pp. 328–335, Jul. 2013.

[2] S. Pai, M. Meingast, T. Roosta et al., "Transactional confidentiality in sensor networks," IEEE Security and Privacy, vol. 6, no. 4, pp. 28–35, Jul. 2008.

[3] J. Deng, R. Han, and S. Mishra, "Countermeasures against traffic analysis attacks in wireless sensor networks," in Security and Privacy for Emerging Areas in Communications Networks(SecureComm'05), 2005.

[4] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "Protecting receiver-location privacy in wireless sensor networks," in Proc. of IEEE INFOCOM, 2007.

[5] A. A. Nezhad, D. Makrakis, and A. Miri, "Anonymous topology discovery for multihop wireless sensor networks," in Proc. of the 3rd ACM workshop on QoS and security for wireless and mobile networks, 2007.

[6] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," in Proc. of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS'05), 2005.

[7] Y. Xi, L. Schwiebert, and W. Shi, "Preserving source location privacy in monitoring-based wireless sensor networks," in the 20th Parallel and Distributed Processing Symposium(IPDPS'06), 2006.

[8] K. Mehta, D. Liu, and M. Wright, "Location privacy in sensor networks against a global eavesdropper," in Proc. of the IEEE International Conference on Network Protocols (ICNP'07), 2007.

[9] Y. Xiang, X. Cheng, K. Xing, D.Chen, and M. Song, "Localized flooding backbone construction for location privacyin sensor networks," in Proc. of the 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD'07), 2007.

[10] S. Madden, M. J. Franklin, and J. M. Hellerstein, "Tag: a tiny aggregation service for ad-hoc sensor networks," in Proc. of the 5th symposium on Operating systems design and implementation (OSDI'02), 2002.

[11] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "Spins: security protocols for sensor networks," Wireless Networks, vol. 8, no. 5, pp. 521–534, Sep. 2002.

[12] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, Introduction to Algorithms, 2nd ed. The MIT Press, 2001.